

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

3840 APPLGATE AVE., APT. 501,
CHEVIOT, OH 45211

Case No. **1:20-MJ-00489**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 USC 922(g)(1)	Felon in possession of firearm or ammunition

The application is based on these facts:

See attached affidavit of ATF Special Agent Edward Schaub

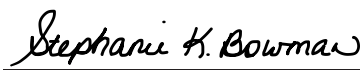
- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Edward Schaub, Special Agent, ATF
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ In person (specify reliable electronic means).

Date: Jul 8, 2020


Judge's signature

City and state: Cincinnati, Ohio

Stephanie K. Bowman, U.S. Magistrate Judge
Printed name and title



ATTACHMENT A

Property to be searched

The property to be searched is 3840 APPLEGATE AVE., APT. 501, CHEVIOT, OH 45211, further described as an apartment within the “Dina Towers” apartment complex at 3850 Applegate Avenue in Cheviot, Ohio. The Dina Towers complex is a light-brown brick building with dark-brown lanais.



ATTACHMENT B

Property to be seized

1. Any and all black pants with a red stripe on the leg;
2. All cellphones, mobile phones, and smartphones belonging to or used by DARIAS JACKSON (hereafter, any “Phone”);
3. To the extent contained on any Phone seized from the PREMISES, all records relating to violations of **18 U.S.C. § 922(g)(1)**, those violations involving DARIAS JACKSON and occurring on or about September 19, 2019, including records and information relating to:
 - a. The shooting of A.W. on or about September 19, 2019, near Groesbeck Road in Cincinnati, Ohio, including any communications relating to the incident;
 - b. The possession of a firearm and ammunition by Darias JACKSON;
 - c. Communications between Darias JACKSON and A.W.;
 - d. Evidence indicating how and when the Phone was accessed or used, to determine the chronological and geographic context of access and use as it relates to the crime under investigation and the Phone’s user;
 - e. Evidence indicating the Phone user’s state of mind as it relates to the crime under investigation; and
 - f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.
4. For any Phone whose seizure is otherwise authorized by this warrant:

- a. evidence of who used, owned, or controlled the Phone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the Phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the Phone was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the Phone user;
- e. evidence indicating the Phone user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the Phone of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Phone;

- h. evidence of the times the Phone was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the Phone;
- j. documentation and manuals that may be necessary to access the Phone or to conduct a forensic examination of the Phone;
- k. records of or information about Internet Protocol addresses used by the Phone;
- l. records of or information about the Phone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data).

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF:
3840 APPLGATE AVE., APT. 501,
CHEVIOT, OH 45211

Case No. **1:20-MJ-00489**

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41
FOR A WARRANT TO SEARCH AND SEIZE**

I, Edward Schaub, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 3840 APPLGATE AVE., APT. 501, CHEVIOT, OH 45211 (the “**PREMISES**”), further described in Attachment A, for the things described in Attachment B.

2. I have been employed with the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) as a Special Agent since September of 2014 and am currently assigned to the ATF Organized Crime Squad. I am a graduate of the Criminal Investigator Training Program and Special Agent Basic Training in Glynco, Georgia. Prior to becoming a Special Agent, I was a Hopkinsville Kentucky Police Officer for eight years and was an ATF Task Force Officer assigned to the Western Kentucky Gun Crimes Task Force in Christian County, Kentucky. I am a graduate of the Department of Criminal Justice Training Center in Richmond, Kentucky. During my employment with ATF, I have been involved in numerous investigations of violations of federal and state criminal laws resulting in multiple successful prosecutions.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

A. On September 19, 2019, the Victim was shot nine times in the parking lot outside an apartment on Groesbeck Road in Cincinnati.

4. At approximately 3:09 am on September 19, 2019, a 911 caller reported that a victim (the "Victim," later identified as A.W.), had been shot near an address on Groesbeck Road in Cincinnati, Ohio. While officers were on their way, they received reports that someone had recently arrived at the hospital suffering from multiple gunshot wounds.

5. Officers located nine 9 mm casings and blood in the parking lot in front of the apartment on Groesbeck Road. The ammunition associated with these casings was manufactured outside the State of Ohio.

6. Shortly after his/her arrival at the hospital, the Victim was taken into surgery and was unable to provide any statements to officers for several days.

B. On October 2, 2019, the Victim identified JACKSON as the shooter.

7. On October 2, 2019, when shown a 6-pack of photographs, the Victim identified Darias JACKSON as the shooter and said he/she had known JACKSON for many years.

8. At the time of the shooting on September 19, 2019, JACKSON was on federal supervised release in connection with his 2013 conviction for Conspiracy to Possess with Intent to Distribute 1,000 Kilograms or More of Marijuana in violation of 21 U.S.C. §§ 846

and 841(a)(1) and (b)(1)(A), a Class A felony punishable by more than one year in prison.

JACKSON was sentenced to 50 months' imprisonment for that offense.

C. On October 31, 2019, the Victim recanted his/her statement under suspicious circumstances.

9. On October 31, 2019, a notary public for the hospital where the Victim was being treated was called to the Victim's room to notarize a statement in which he/she recanted his/her identification of JACKSON as the shooter.

10. Upon entering, the notary saw six people in the room: the Victim, who was sitting in his/her bed with his/her legs dangling over the side; three individuals on a love seat who the notary believed were likely the Victim's parents and a sibling; and two unknown males in the back of the room. The notary stated that the two men in the back of the room brought the typewritten affidavit to her. The Victim told the notary that he/she had read the affidavit. The notary then asked three questions to determine whether the Victim was competent to sign the affidavit ("Who is the president of the United States?" "Where are you?" and "What is today's date?"). After receiving satisfactory responses, the notary reviewed the affidavit with the Victim and noted to him/her that it appeared the Victim was recanting a previous statement. The Victim responded that he/she was recanting because the person the Victim had accused was the Victim's cousin and it was the first name he/she had thought of after the shooting and that was why he/she said the name originally. According to the notary, the Victim stated, "He's my boy; it was not him." When one of the individuals the notary believed were the Victim's parents asked what the Victim was signing, the Victim responded that it was just paperwork for the hospital.

11. The Victim signed the affidavit, and the notary notarized it. As soon as the document was notarized, the two men in the back of the room stepped forward, took the signed statement, and walked out of the room.

D. On January 8, 2020, the Victim reaffirmed that JACKSON was the shooter.

12. In a telephone interview on January 8, 2020, the Victim again identified JACKSON as the shooter, saying that he/she had been on a substantial amount of pain medicine when he/she signed the affidavit on October 31, 2019.

E. A video taken moments before the shooting appears to show the Victim and JACKSON in an aggressive verbal confrontation.

13. After the shooting, but before the Victim was medically stable and could be interviewed, law enforcement received anonymous tips that someone had taken video of a confrontation between the Victim and JACKSON shortly before the shooting.

14. Law enforcement later obtained a copy of the video, which shows two individuals who strongly resemble the Victim and JACKSON in an aggressive verbal confrontation. The two individuals appear to be standing in the parking lot outside the Island Breeze Apartments on Groesbeck Road, near where the Victim was shot.

15. The video's metadata show that the video was taken at 3:06 am on September 19, 2019—approximately three minutes before the 911 call reporting that the Victim had been shot. The video also partially shows a vehicle that is consistent in appearance with a vehicle registered to JACKSON; the person who appears to be JACKSON is sitting on that vehicle in parts of the video. Because the video appears to have been taken from inside an apartment, while the two individuals were outside in the parking lot, the individuals' words cannot be clearly heard.

16. The video shows that the person who appears to be JACKSON is wearing a pair of black pants with a red stripe down the side of the leg.



F. Calls between JACKSON and his significant other contain evidence that JACKSON's cellphones are at the PREMISES.

17. An arrest warrant was eventually issued for JACKSON; however, JACKSON self-surrendered on October 4, 2019, before the arrest warrant was executed. At the time of his surrender, JACKSON did not have a cellphone on his person.

18. I listened to certain jail calls JACKSON made after his arrest, including calls on which JACKSON spoke with a woman who was using a phone number ending in 5895 (the "5895 Phone").

19. In February 2020, when asked about phone numbers relating to JACKSON, JACKSON's probation officer reported that J.B., JACKSON's significant other, had contacted him using the 5895 Phone. I therefore believe that the 5895 Phone is used by J.B.

20. On one call between JACKSON and J.B., who was using the 5895 Phone, JACKSON asserted that J.B. had been looking through his phone. What follows is a partial transcript of the relevant portions of that call. These transcripts are based on my best attempt to understand the words being said and convey what I believe to be the substance of the call; however, the poor audio quality made it difficult to determine the exact words being said:

JACKSON:	So, why you was going through my phone?
J.B.:	I told you: I was bored.
JACKSON:	You keep saying that [laughs]
J.B.:	I mean, I could have lied and said that somebody told me [U/I] I could have lied and made up a story [laughter] It's just making me feel better, because [U/I] my mind be [U/I]
JACKSON:	Oh, so you activated my Facebook?
J.B.:	You hear me?
JACKSON:	Huh?
J.B.:	I said you hear me claiming to get an Instagram [U/I]
JACKSON:	How'd you get in Facebook?
J.B.:	Because when you download the app, or some app... [laughs]

21. Based on my training and experience and knowledge of this case, including the fact that JACKSON did not have a cellphone on him when he self-surrendered, I believe that on this portion of the call, JACKSON and J.B. were discussing how JACKSON had left his phone with J.B., and J.B. had gone through it.

22. Later on the same call, JACKSON and J.B. again appeared to be discussing how J.B. was looking through the contents of JACKSON's phone:

JACKSON: I'm saying, you're talking about something that's super old, though, babe.

J.B.: No, it's not old [U/I] You was just texting her at the last [U/I]. And that's just what I've seen. And you cut off half of the messages, so I ain't gonna tell [U/I] what y'all was talking about beforehand.

JACKSON: I cut off half the messages?

J.B.: Yeah, like you just [U/I] the part that you wanted [U/I]

JACKSON: Go ahead

[. . .]

J.B.: And why you gon' be my baby daddy? [U/I]

JACKSON: [U/I] left you, left [U/I] phone.

[cross-talk/noise in background]

J.B.: And I was so surprised, because [U/I] the first time. You gave it to your brother.

JACKSON: I mean, I'm saying, like, motherfucker ain't called, nothing', like --

J.B.: I did tell you somebody called. So who told him --

JACKSON: Yeah, but that's, that's out of the blue. You know that. I just told you.

23. Based on my training and experience and knowledge of this case, I believe that in this portion of the call, J.B. was asserting that she had reviewed text messages on JACKSON's

phone and had noticed that he had deleted “half of the messages” that JACKSON had exchanged with another woman.

24. On a later call, JACKSON and J.B. had the following exchange:

JACKSON: I told you to get on my Facebook. Why you didn’t get on – why you didn’t type my name in it and see what’s going on?

J.B.: [U/I]

JACKSON: My page ain’t private. You can go on there and look and see what’s going on. You do it any other time [laughs]

J.B.: Nuh-uh; I stopped. [U/I] You caught me. [U/I]
[....]

J.B. What’s your password again?

JACKSON: Girl, you already got it. I said log in on yours

25. Based on my training and experience and knowledge of this case, including the other call described above, I believe that on this call, J.B. and JACKSON were discussing how J.B. has been able to access JACKSON’s Facebook account through his phone.

26. On another call, JACKSON said to J.B.: “You got my phone right there? Do me a favor.” When J.B. asked “Which one?”, JACKSON responded, “The white and black one.”

27. Based on the foregoing calls, I believe that JACKSON gave J.B. multiple cellphones for safekeeping before self-surrendering. JACKSON has been in custody since the time these calls were made. Accordingly, I believe there is probable cause to believe that J.B. still has custody of JACKSON’s phones.

28. On July 7, 2020, I asked J.B. where she lived; she told me that she lived at the **PREMISES.**

29. According to JACKSON's probation officer, on or about October 1, 2019, JACKSON said that he and J.B. were moving to the **PREMISES** on or about October 5, 2019.

30. According to JACKSON's probation officer, JACKSON and J.B. have been dating since high school. They have three children together, the youngest being born during JACKSON's current incarceration.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

31. As described above and in Attachment B, this application seeks permission to search for cellphones, mobile phones, and smart phones (all forms of computers and/or storage media) that might be found on the **PREMISES**, as well as relevant records and information that might be stored on those devices. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. *Probable cause.* I submit that if a cellphone, mobile phone, or smart phone is found on the **PREMISES**, there is probable cause to believe that relevant records will be stored on that device for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers (including cellphones, mobile phones, and smartphones) were used, the purpose of

their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **PREMISES** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of

session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a

digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

34. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the

warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

35. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

36. Because evidence suggests that multiple individuals live at the PREMISES, including J.B., it is likely that the **PREMISES** will contain storage media that are predominantly

used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

37. I submit that this affidavit supports probable cause for a warrant to search the **PREMISES** described in Attachment A and seize the items described in Attachment B.

//

//

//

//

//

//

//

//

//

//

//

//

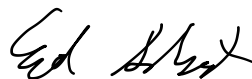
//

//

REQUEST FOR SEALING

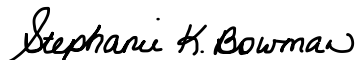
38. I respectfully request that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary because the items and information to be seized are relevant to an ongoing investigation. Although the target of this investigation, JACKSON, is aware that the case is being investigated, he is not aware of the full scope of the government's attempts to obtain evidence in this case. If JACKSON learns that the government continues to investigate the shooting, and in particular if he learns of the government's intent to search J.B.'s residence, he may direct J.B. to dispose of the evidence sought by this search warrant, or other evidence about which the government is not yet aware. For these reasons, premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,



EDWARD SCHAUB
Special Agent
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Attested to by the Applicant in accordance with Fed. R. Crim. P. 4.1 this 8th day of July, 2020.



HON. STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A

Property to be searched

The property to be searched is 3840 APPLEGATE AVE., APT. 501, CHEVIOT, OH 45211, further described as an apartment within the “Dina Towers” apartment complex at 3850 Applegate Avenue in Cheviot, Ohio. The Dina Towers complex is a light-brown brick building with dark-brown lanais.



ATTACHMENT B

Property to be seized

1. Any and all black pants with a red stripe on the leg;
2. All cellphones, mobile phones, and smartphones belonging to or used by DARIAS JACKSON (hereafter, any “Phone”);
3. To the extent contained on any Phone seized from the PREMISES, all records relating to violations of **18 U.S.C. § 922(g)(1)**, those violations involving DARIAS JACKSON and occurring on or about September 19, 2019, including records and information relating to:
 - a. The shooting of A.W. on or about September 19, 2019, near Groesbeck Road in Cincinnati, Ohio, including any communications relating to the incident;
 - b. The possession of a firearm and ammunition by Darias JACKSON;
 - c. Communications between Darias JACKSON and A.W.;
 - d. Evidence indicating how and when the Phone was accessed or used, to determine the chronological and geographic context of access and use as it relates to the crime under investigation and the Phone’s user;
 - e. Evidence indicating the Phone user’s state of mind as it relates to the crime under investigation; and
 - f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.
4. For any Phone whose seizure is otherwise authorized by this warrant:

- a. evidence of who used, owned, or controlled the Phone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the Phone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the Phone was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the Phone user;
- e. evidence indicating the Phone user’s state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the Phone of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Phone;

- h. evidence of the times the Phone was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the Phone;
- j. documentation and manuals that may be necessary to access the Phone or to conduct a forensic examination of the Phone;
- k. records of or information about Internet Protocol addresses used by the Phone;
- l. records of or information about the Phone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data).